(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 November 2006 (23.11.2006)

PCT

(10) International Publication Number
WO 2006/124160 A3

(51) International Patent Classification:
H04L 9/00 (2006.01)

(21) International Application Number:
PCT/US2006/013795

(22) International Filing Date: 12 April 2006 (12.04.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

05/04779	12 May 2005 (12.05.2005)	FR
11/203,939	15 August 2005 (15.08.2005)	US

(71) Applicant *(for all designated States except US)*: **ATMEL CORPORATION** [US/US]; 2325 Orchard Parkway, San Jose, California 95131 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **DUPAQUIS, Vincent** [FR/FR]; 22 Residence Victor Savine, F-13120 Biver (FR). **DOUGUET, Michel** [FR/FR]; 152 Avenue De Mazargues, F-13008 Marseille (FR).

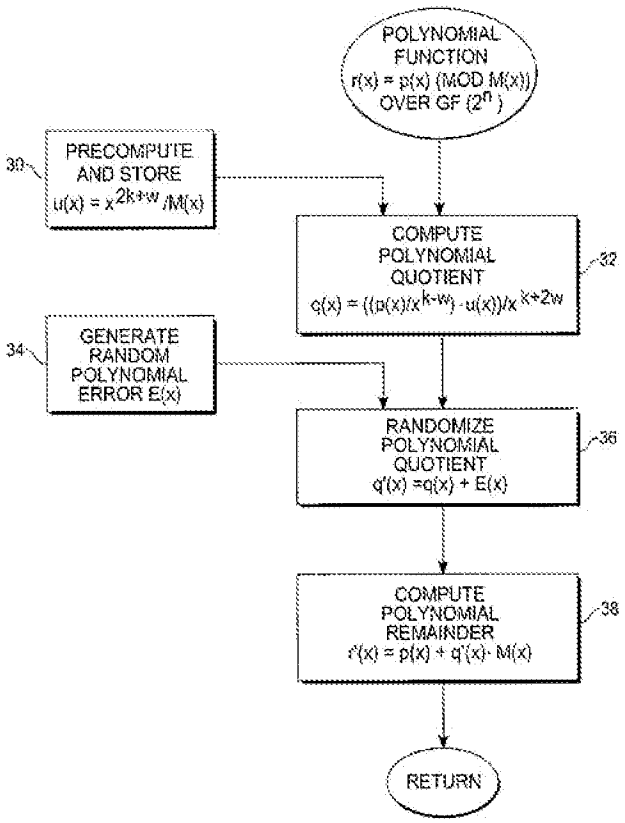
(74) Agent: **SCHNECK, Thomas**; Schneck & Schneck, P.O. Box 2-E, San Jose, California 95109-0005 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: RANDOMIZED MODULAR POLYNOMIAL REDUCTION METHOD AND HARDWARE THEREFOR



(57) Abstract: A cryptographically secure, computer hardware-implemented binary finite-field polynomial modular reduction method estimates (32) and randomizes (36) a polynomial quotient q' (x) used for computation of a polynomial remainder. The randomizing error E (x) injected into the approximate polynomial quotient q (x) is limited to a few bits, e.g. less than half a word. The computed (38) polynomial remainder r' (x) is congruent with but a small random multiple of the residue r (x), which can be found by a final strict binary field reduction by the modulus M (x). In addition to a computational unit (10) and operations sequencer (16), the computing hardware also includes a random or pseudo-random number generator (20) for producing the random polynomial error. The modular reduction method thus resists hardware cryptoanalysis attacks, such as timing and power analysis attacks.

WO 2006/124160 A3

Declarations under Rule 4.17:

- *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*
- *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

- *with international search report*
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
13 December 2007

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 06/13795

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8): H04L 9/00 (2007.01)
USPC: 713/174
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
USPC: 713/174

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC: 713/165

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
pubWEST(PGPB,USPT,EPAB,JPAB); DialogPRO(Engineering); Google Scholar.
Search terms: cryptographically secure, computer hardware, finite-field, elliptical curve, polynomial, randomize

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2002/0055962 A1 (SCHROEPPEL) 09 May 2002 (09.05.2002) entire document, especially para [0044]-[0050], [0078] and FIG.3.	1-11
A	Morales-Sandoval, et al. On the hardware design of an elliptic curve cryptosystem. In Computer Science, 2004. ENC 2004. Proceedings of the Fifth Mexican International Conference in, Posted online 2004-10-18 08:49:27.0 (retrieved on 2007-06-12). Retrieved from the internet: <URL: http://ccc.inaoep.mx/~cferegrino/Publicaciones/articulos/OntheHardwareDesign%20of%20an%20Elliptic%20Curve%20Criptosystem_ENC04_MiguelMorales.pdf >	1-11

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 June 2007 (12.06.2007)	19 OCT 2007
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (April 2005)